



**Tactics, Techniques, and Procedures**  
**for**  
**Activating your “PIV Authentication” Certificate**  
**for use with**  
**DoD Enterprise Email**

**13 July 2015**

**DOD EE TTP-6**  
**Version 2.1**

## EXECUTIVE SUMMARY

This Tactics, Techniques, and Procedures (TTP) document describes the processes that end users with a “dual persona” to expose the PIV Authentication Certificate on their Common Access Card(s), which they will then use to authenticate to DoD Enterprise Email (EE).

## DOCUMENT REVISIONS LIST

VERSION	DATE	DESCRIPTION OF CHANGES	ORGANIZATION
1.0	23 Jan 13	Initial (Army) Version	HQDA CIO/G6 (LTC Barclay)
1.1	23 Jan 15	Updates based on RSS changes, updated screenshots, adding trusted sites to Java security	PO EE, PEO EIS, (Peter Barclay)
1.2	24 Feb 15	Additional of clarification on why PIV Auth certs are required	DISA, DMDC, PEO EIS
2.0	15 May 15	Beta site functionality move to main RSS site. URL and screenshots updated	DMDC, Army PEO EIS – PO EE
2.1	13 Jul 15	Correction of the highlighted portion of a screenshot	PO EE

## TABLE OF CONTENTS

1	The PIV Authentication Certificate Activation Process .....	4
2	Step 1: Ensure that your computer will trust the websites.....	4
3	Step 2: Access RAPIDS Self Service portal.....	6
4	Step 3: Make the Certificates Available to Windows .....	13
5	Why is the PIV Authentication certificate required?.....	16
6	What can be done to make the PIV Authentication requirement “go away”? ...	16

## TABLE OF FIGURES

Figure 1.	Java icon in the Control Panel .....	4
Figure 2.	The Java Control Panel .....	4
Figure 3.	Security tab in the Java Control Panel .....	5
Figure 4.	Exception Site List .....	6
Figure 5.	Adding sites to the Exception Site List .....	6
Figure 6.	RAPIDS Self Service website .....	7
Figure 7.	Consent to Monitor .....	7
Figure 8.	CAC Login to RSS .....	8
Figure 9.	Selecting Authentication certificate .....	8
Figure 10.	Select the correct CAC and click “Activate PIV Certificate” .....	9
Figure 11.	Ready to activate PIV Authentication cert .....	9
Figure 12.	Reading data from the CAC – 0%.....	10
Figure 13.	Accepting the Java applet.....	10
Figure 14.	Confirm you want to update the CAC.....	11
Figure 15.	Starting PIV Activation request to Post Issuance Portal .....	11
Figure 16.	Request to the LCM User Portal .....	12
Figure 17.	Enter CAC PIN.....	12
Figure 18.	Activating PIV Authentication Certificate .....	12
Figure 19.	Confirmation the CAC has been updated.....	13
Figure 20.	Launching ActivClient .....	13
Figure 21.	Forgetting state for all cards.....	14
Figure 22.	Opening My Certificates.....	14
Figure 23.	Verifying all four certificates are visible .....	15
Figure 24.	Making certificates available to Windows .....	15

## 1 The PIV Authentication Certificate Activation Process

Being able to use a PIV Auth cert is a two step process. Activate the PIV Auth certificate using RAPIDS Self Service (RSS), and then make the certificate available to Windows.

The RAPIDS Self Service portal has many features and capabilities, but actually has two different options for activating the PIV Auth certificate. Based on past experience with the original software, RSS has developed a new PIV Auth activation capability with more robust functionality and performance. This document is about using that new capability.

**IMPORTANT NOTE:** The primary reason for activating the PIV Authentication certificate is that each dual persona user **must use** the PIV Auth certificate ***to authenticate*** to Enterprise Email. As a dual persona individual, **you will always use this certificate to authenticate to Enterprise Email.**

## 2 Step 1: Ensure that your computer will trust the websites.

The new PIV Auth activation capability makes use of some enhanced Java features and we have found that most DoD computers don't trust the DMDC websites providing the Java application. Although you can set either IE or Java to trust the websites, it is simplest to have Java trust those sites.

- 1) Open the "Control Panel" on your computer and then double-click the Java icon to open the Java Control Panel.

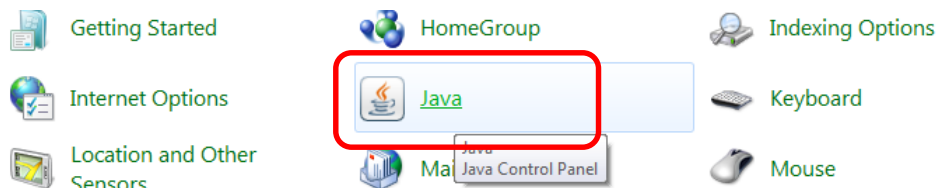


Figure 1. Java icon in the Control Panel

- 2) On the Java Control Panel, select the "Security" tab.

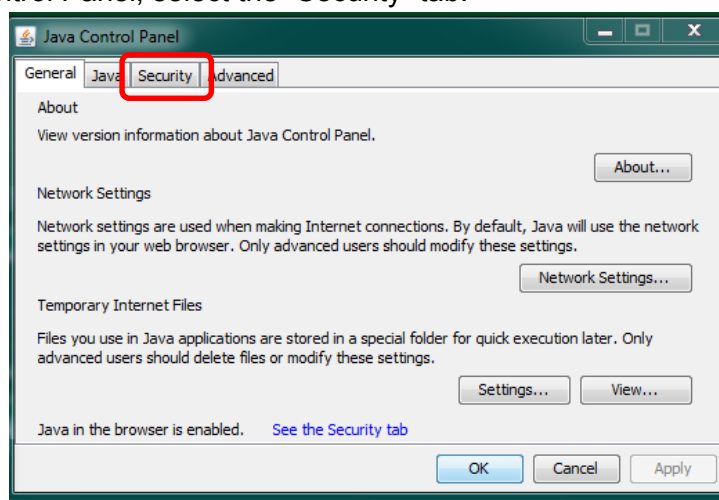
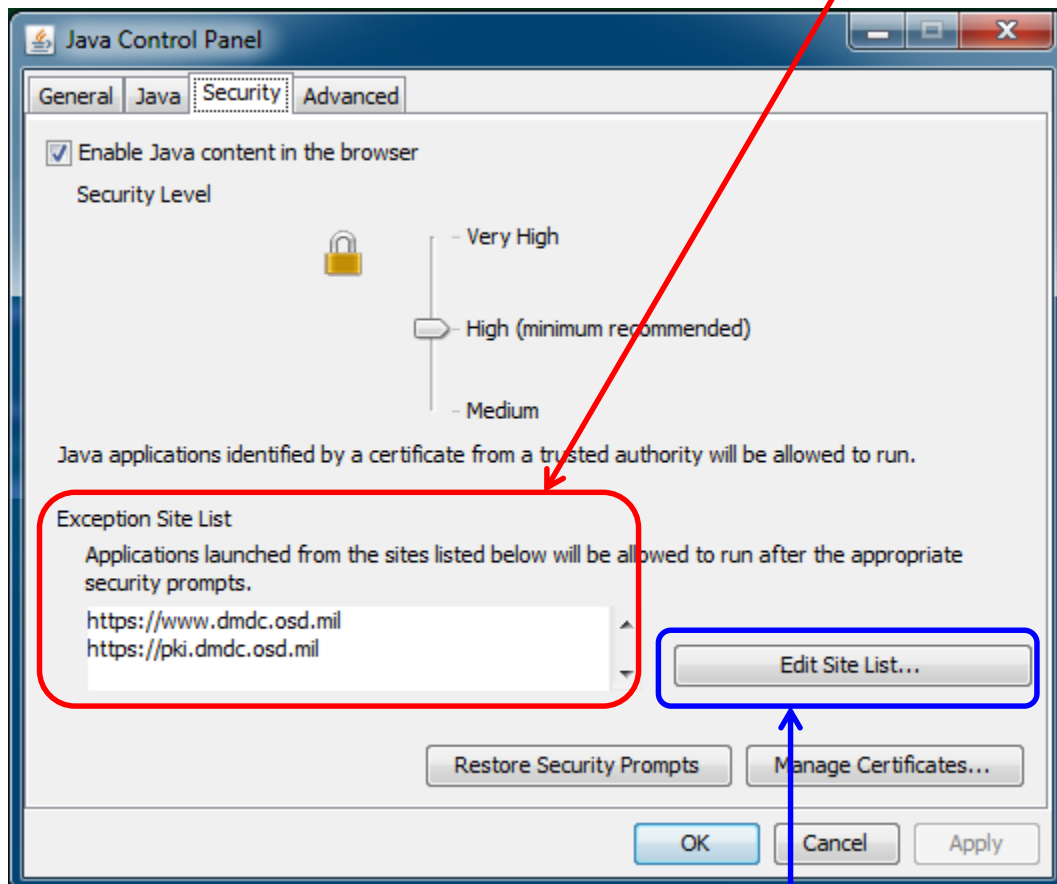


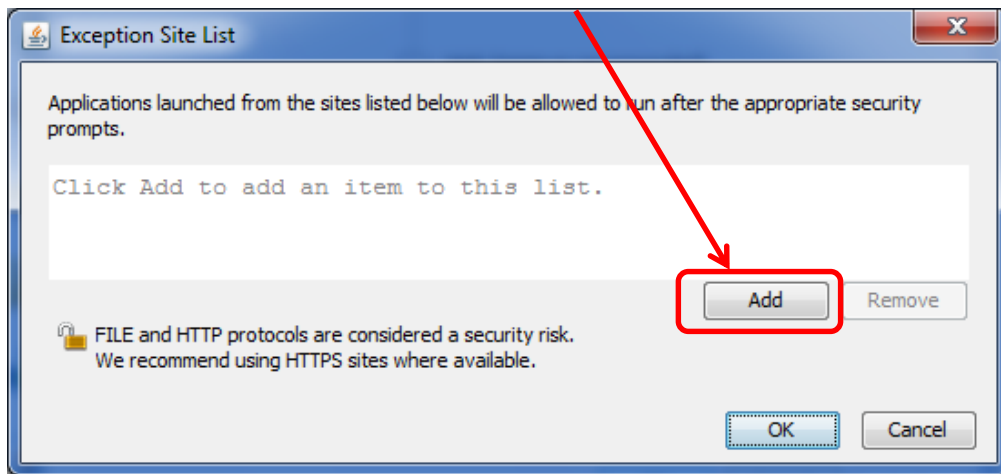
Figure 2. The Java Control Panel

- 3) On the Security tab, make sure the following two sites are in the “Exception Site List” area:
- <https://www.dmdc.osd.mil>
  - <https://pki.dmdc.osd.mil>



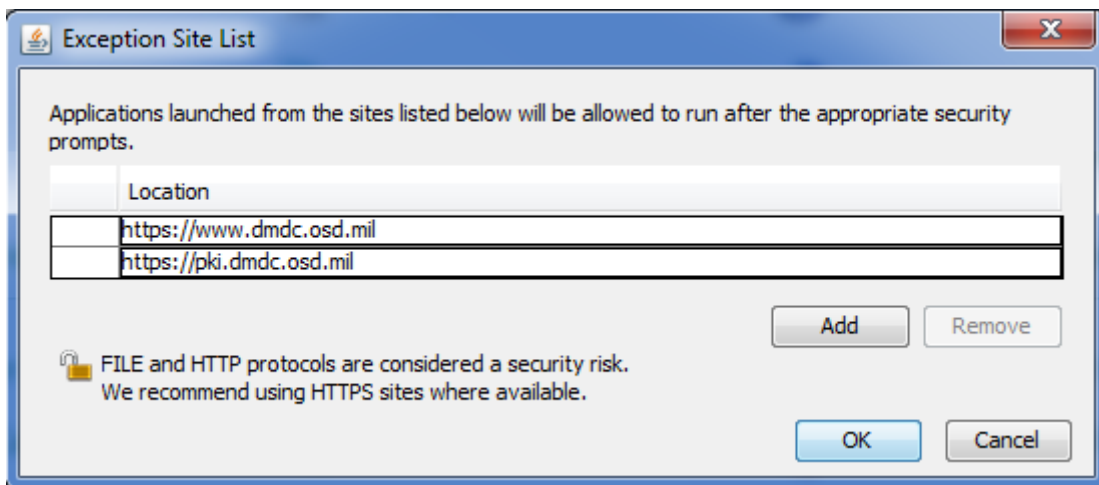
**Figure 3. Security tab in the Java Control Panel**

- 4) If those two sites are not listed, They will need to be added. Click the “<Edit Site List...>” button.
- 5) On the Exception Site List window, click the <Add> button.



**Figure 4. Exception Site List**

- 6) Add the two URLs (site addresses) to the Location list, clicking the **<Add>** button to add each new line in the table.



**Figure 5. Adding sites to the Exception Site List**

- 7) Click **<OK>** once both site addresses are listed and then click **<OK>** to close the Java Control Panel.

### **3 Step 2: Access RAPIDS Self Service portal**

- 1) Ensure that your CAC is inserted into its reader and sign on to the RAPIDS Self Service Portal by going to: [https://www.dmdc.osd.mil/self\\_service/](https://www.dmdc.osd.mil/self_service/)

2) When the RSS website opens click the <Sign In> button.

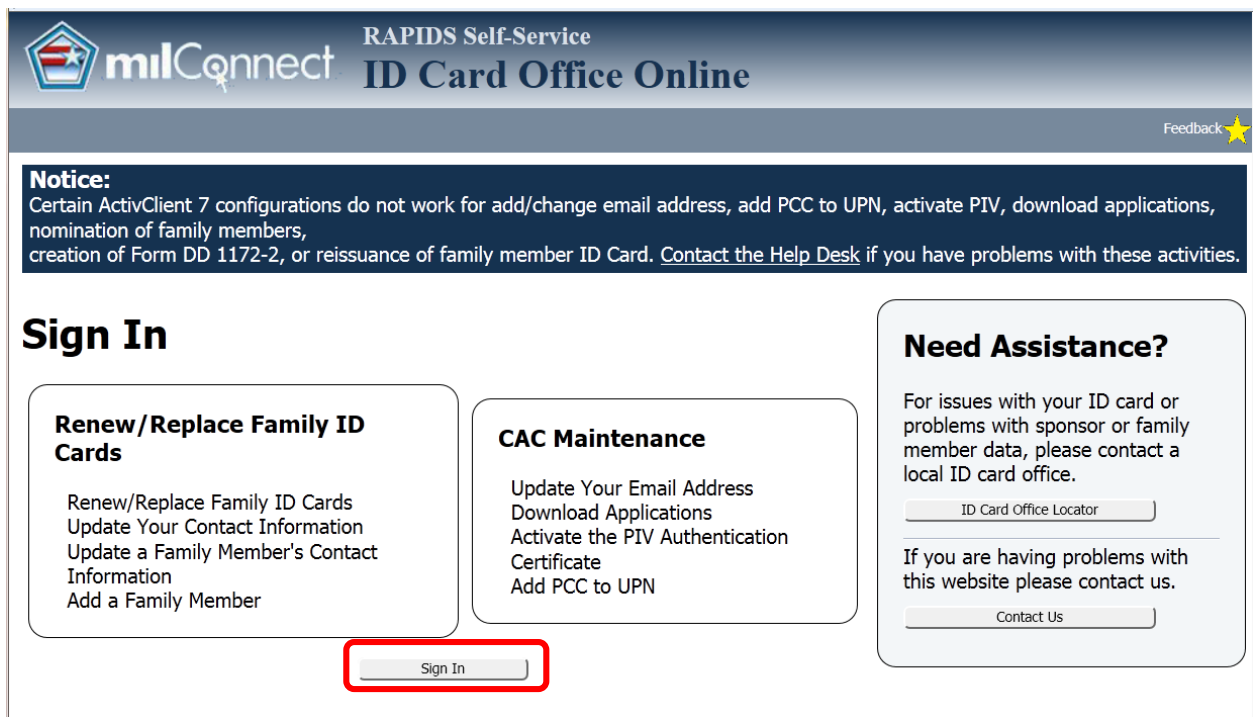


Figure 6. RAPIDS Self Service website

3) Accept the DoD Notice and Self-Service Consent by clicking <OK>

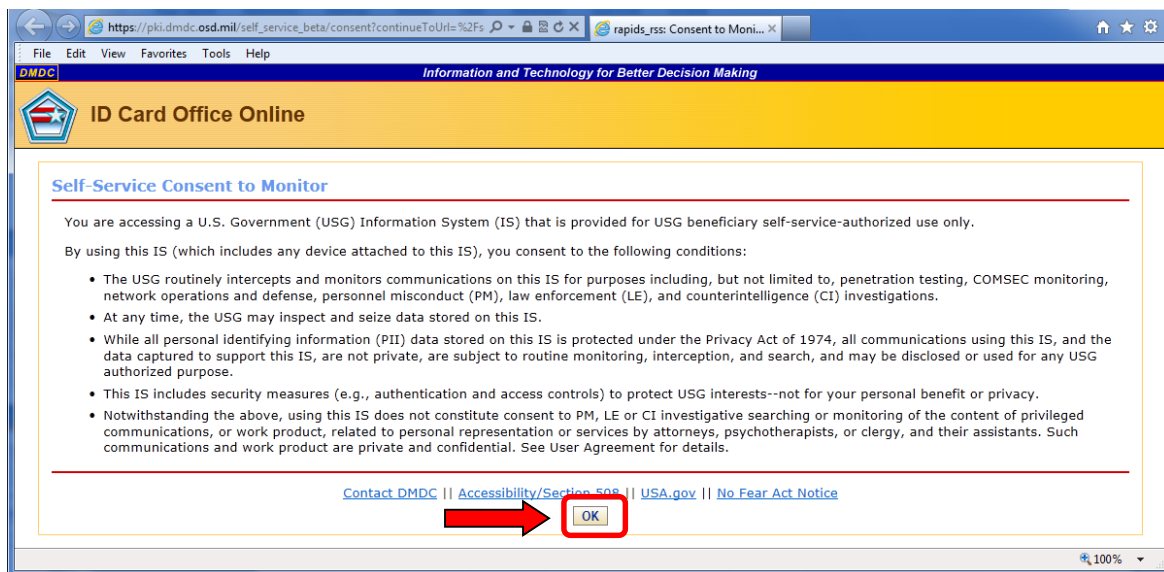


Figure 7. Consent to Monitor

- 4) Click the <Login> button.

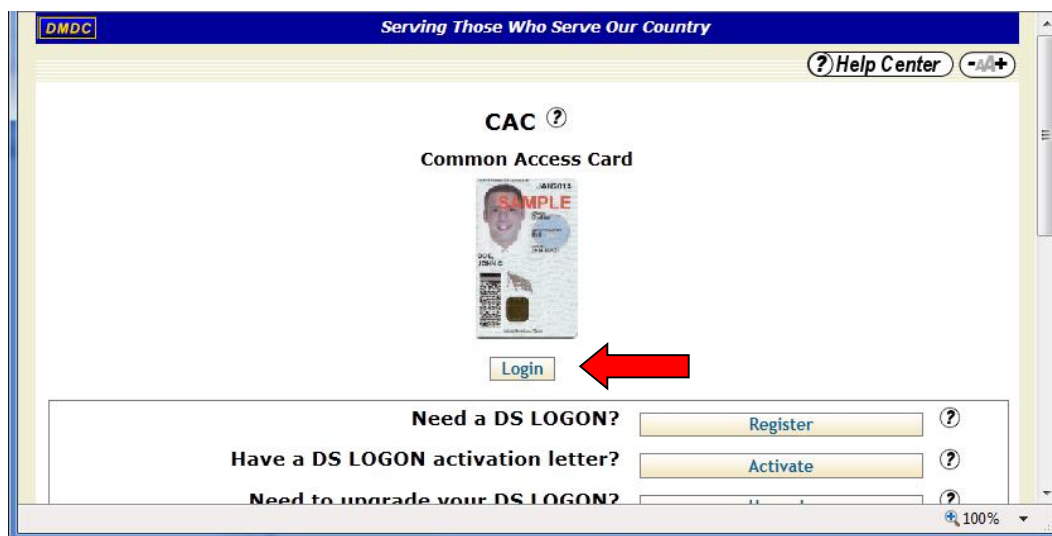


Figure 8. CAC Login to RSS

- 5) When the dialogue box with your certificates pops up, select the "DoD Email CA-xx" certificate and click the <OK> button.

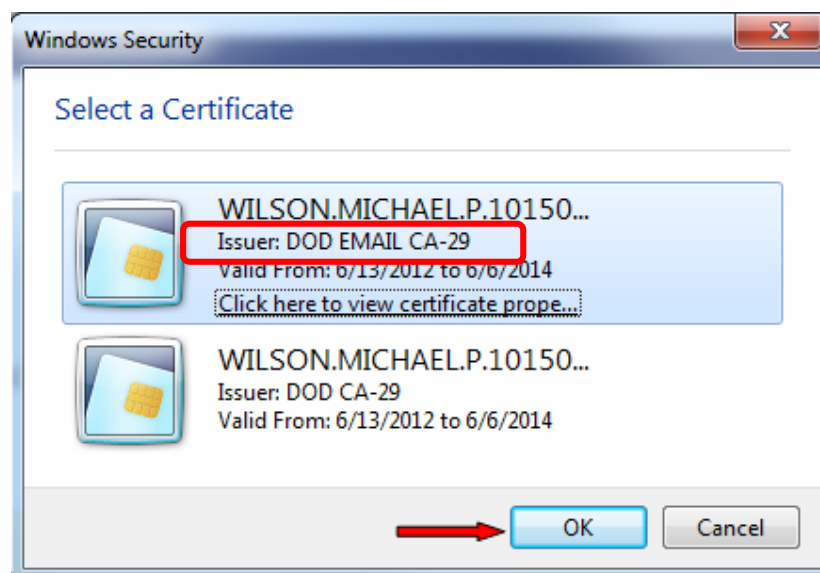


Figure 9. Selecting Authentication certificate

- 6) Once the RAPIDS Self-Service webpage opens for you, select the "<Activate PIV certificate>" for the "persona" you now want to use. A "persona" is the identity of the specific CAC for which you are trying to expose the PIV Auth certificate, such as your military (mil), civilian (civ), contractor (ctr), or other persona

**IMPORTANT NOTE:** The reason for activating the PIV Authentication certificate is that each dual persona user **must use** the PIV Auth certificate ***to authenticate*** to Enterprise Email. As a dual persona individual, **you will always use this certificate to authenticate to Enterprise Email.**

The screenshot shows the 'milConnect ID Card Office Online' interface. The 'CAC Maintenance' section for Donald R. Greenlee JR. (Email: donald.r.greenlee.mil@mail.mil) is displayed. It lists two CACs: one for Reserve (Card Expires 2017Jan15) and one for Civil Service (DoD and Uniformed Service) (Card Expires 2018Feb01). The 'Activate PIV certificate' button for the Civil Service CAC is highlighted with a red box and a red arrow. Other buttons include 'Change CAC Email', 'Download Applications', 'Generate 1172-2', 'Add PCC on UPN', and 'Edit Contact Information'.

Figure 10. Select the correct CAC and click “Activate PIV Certificate”

- 7) Once you click “Activate PIV certificate” you will get a confirmation screen. Click the **<Proceed>** button.

The screenshot shows the 'Activate PIV Certificate' confirmation screen. On the left, a 'SELECTED CARD' is displayed for Donald R. Greenlee JR. (Card Expires FEB2018). The main area contains the text: 'Reading CAC for Activate PIV Certificate. To activate the PIV Authentication certificate, information must be read from your CAC. The PIV Authentication certificate was added in support of FIPS 201. This certificate, in conjunction with the PIV End Point applet, allows access to federal websites which require PIV authentication. This can take several minutes. Please do not refresh the screen or click the browser's back button.' At the bottom, the 'Proceed' button is highlighted with a red box, next to a 'Cancel' button.

Figure 11. Ready to activate PIV Authentication cert

The Java applet will read the CAC.

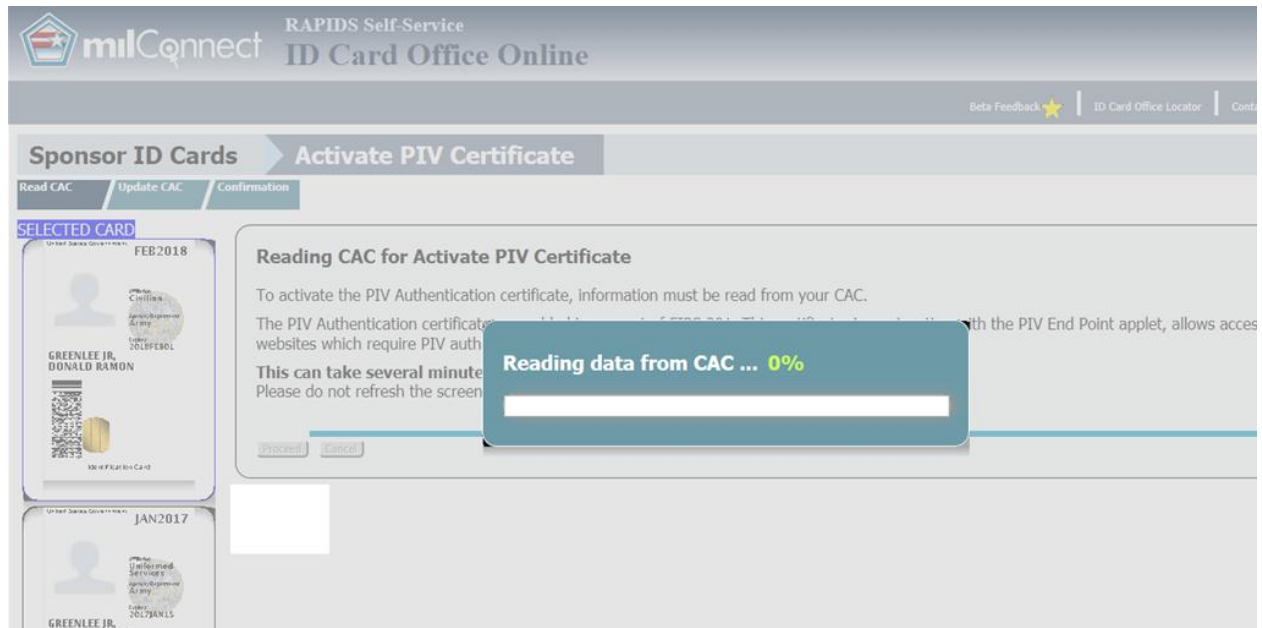


Figure 12. Reading data from the CAC – 0%

- 8) The Java applet from the DMDC ID Card office software will appear and ask for confirmation to execute the applet.

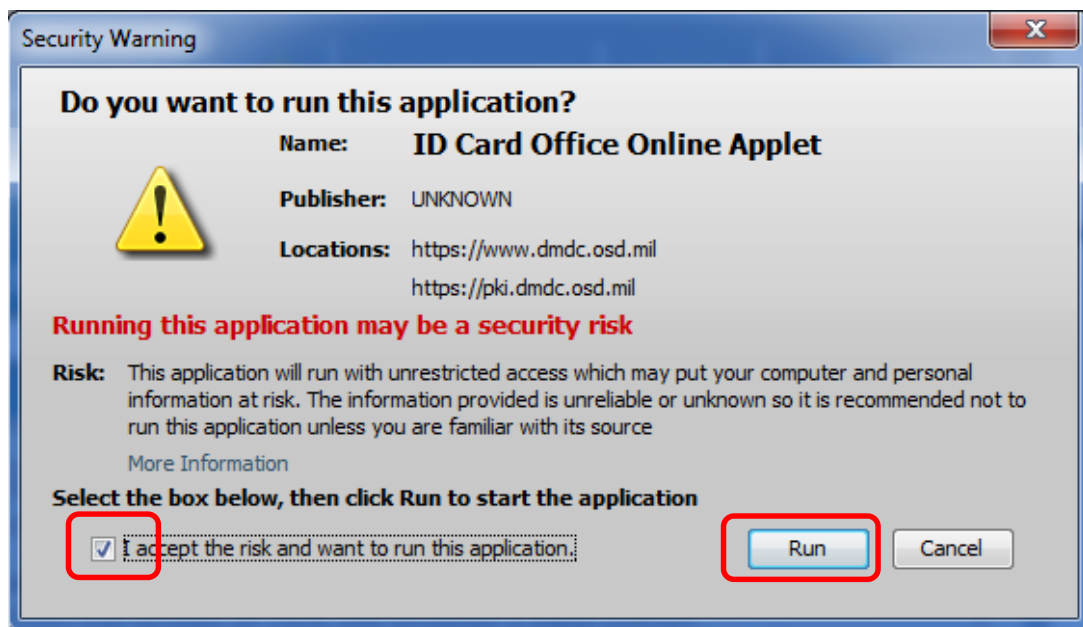


Figure 13. Accepting the Java applet

Check the box for “I accept the risk and want to run this application” and then click "<Run>". to continue when you get the pop-up screen.

Once the Java applet executes, the portal will verify that you want to expose the PIV certificate and update the CAC.

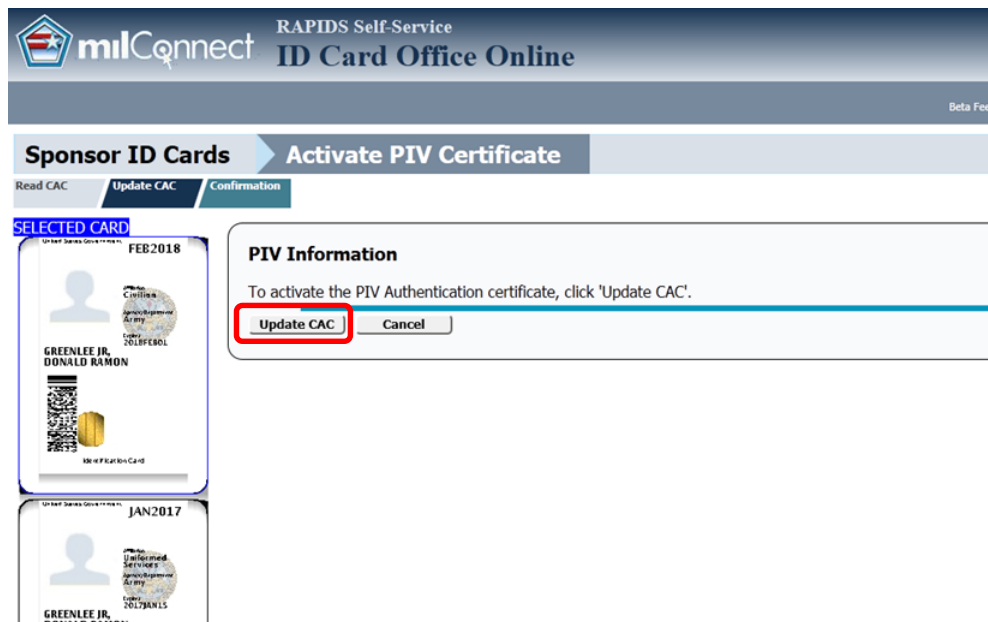


Figure 14. Confirm you want to update the CAC

- 9) DO NOT REMOVE THE CARD FROM THE READER. It can sometimes take a few minutes for the application to read all the details and then updated the CAC, exposing the certification. Be patient.

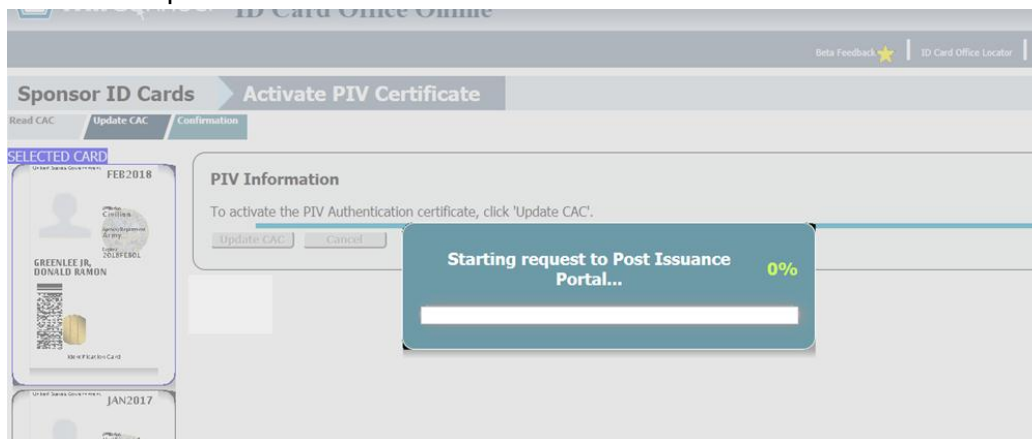
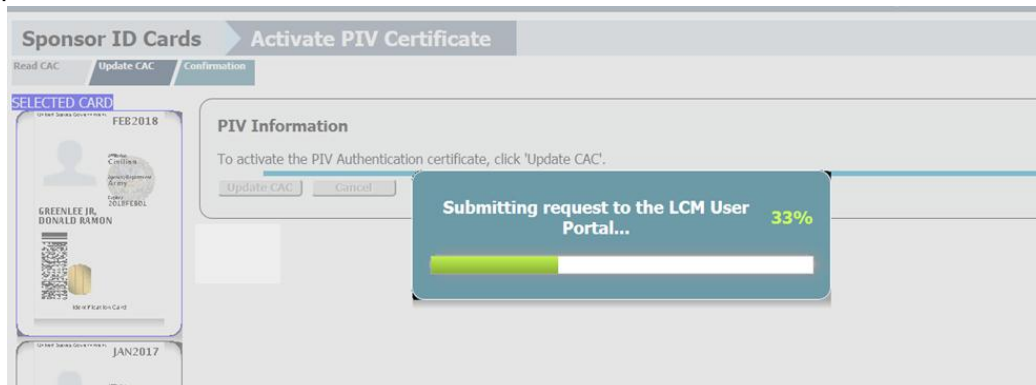


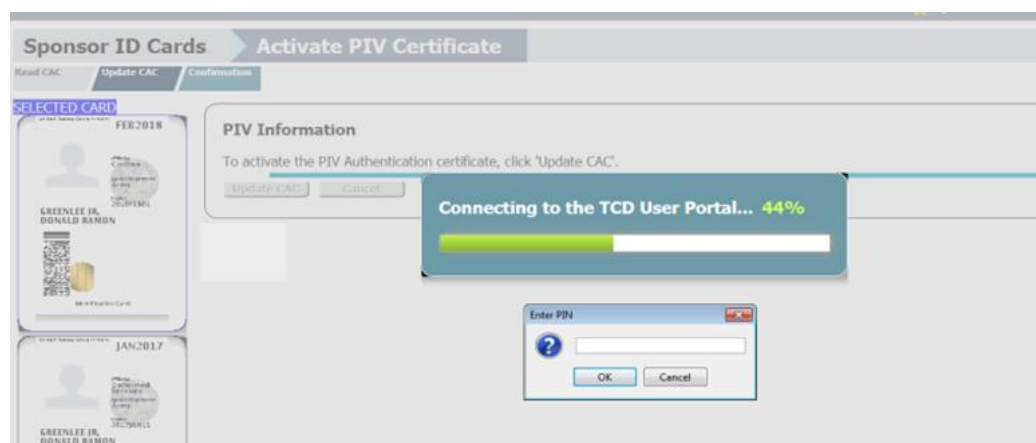
Figure 15. Starting PIV Activation request to Post Issuance Portal

- 10) The application will walk through the process, contacting the portals necessary to complete the process.



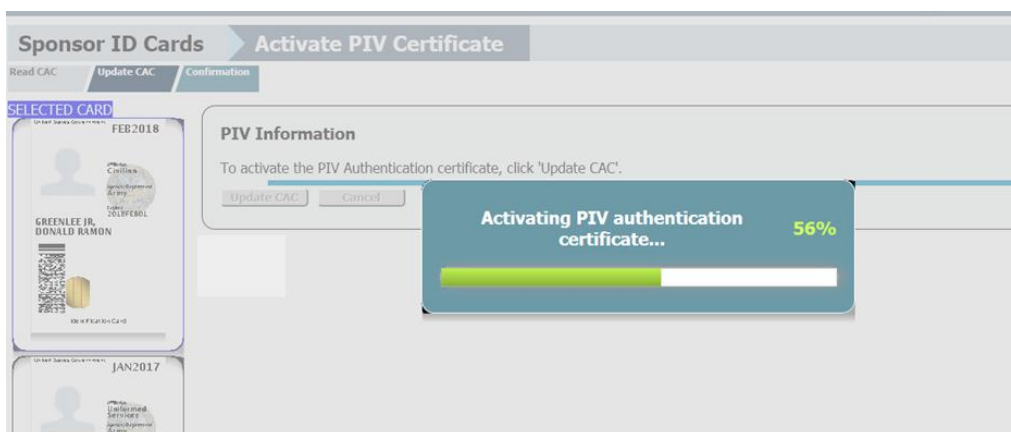
**Figure 16. Request to the LCM User Portal**

There may be occasions when you will need to re-enter your PIN for your CAC. This is normal.



**Figure 17. Enter CAC PIN**

The application will continue and will activate your PIV Authentication certificate.



**Figure 18. Activating PIV Authentication Certificate**

- 11) The application will continue and will complete the activation of your PIV Authentication certificate. When finished, it will notify you that the update is complete.

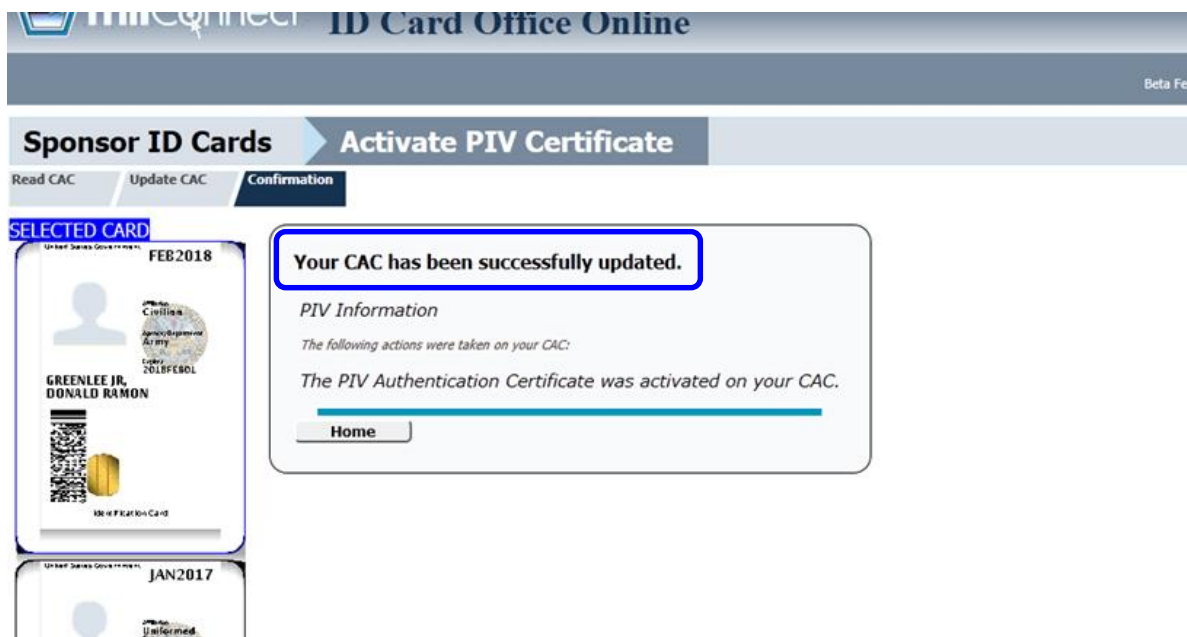


Figure 19. Confirmation the CAC has been updated

- 12) Once the CAC update is complete, remove it from the reader.

**NOTE:** If the “Activate PIV Authentication Certificate” update process failed to run, or the update failed, the user will need to visit their local Defense Enrollment Eligibility Reporting System/RAPIDS (DEERS/RAPIDS) office to obtain a new CAC because the current CAC is too old and does not contain the PIV AUTH certificate.

#### 4 Step 3: Make the Certificates Available to Windows

- 1) Insert your CAC back into the card reader.
- 2) Open **ActivClient** by double clicking the CAC icon in the system tray (bottom right corner of the screen).

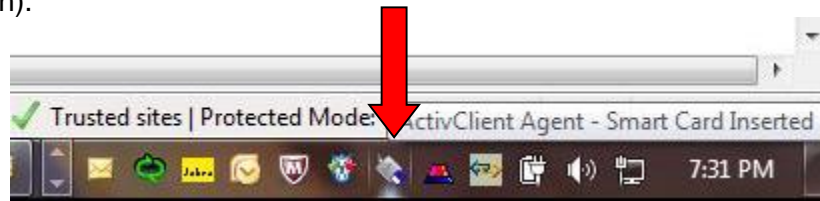


Figure 20. Launching ActivClient

3) In the ActivClient menu, open **<Tools> -- <Advanced> -- <Forget state for all cards>**.



Figure 21. Forgetting state for all cards

4) Now, double click **<My Certificates>**. This will force the card reader to re-read the card.

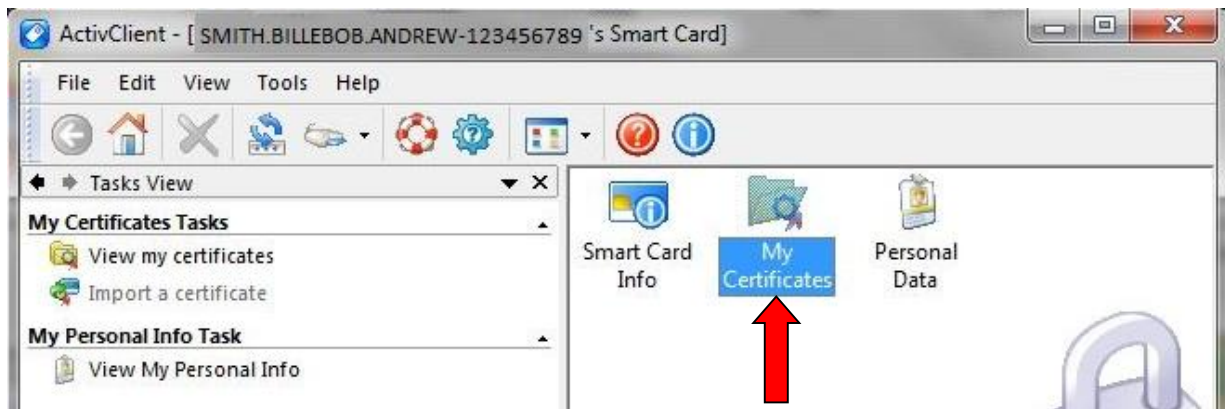


Figure 22. Opening My Certificates

- 5) Ensure that **four certificates** are displayed, one of which is the "PIV AUTH Certificate" like the example below.

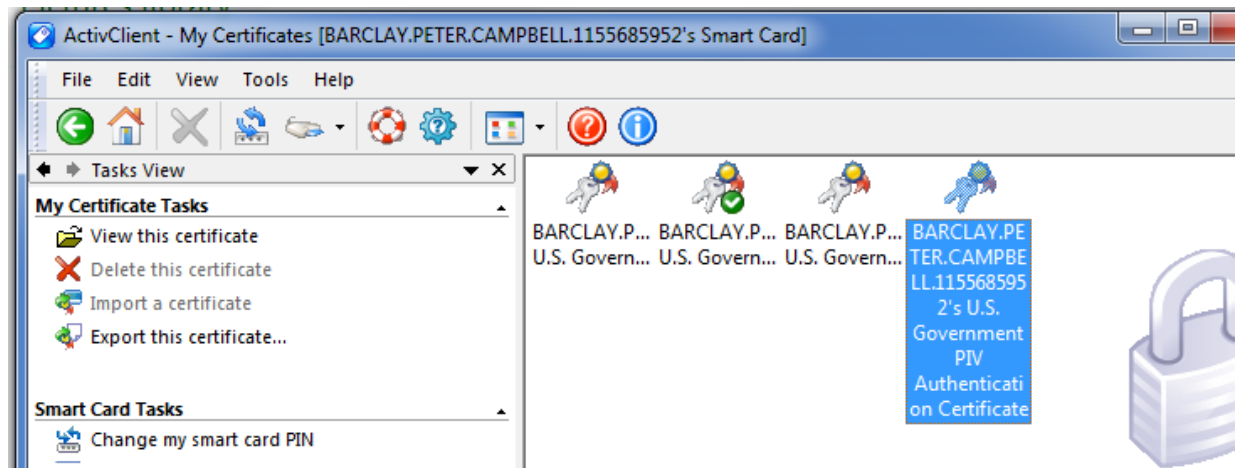


Figure 23. Verifying all four certificates are visible

**NOTE:** If the PIV Authentication Certificate is not displayed in this step, activation did not succeed. The user will need to visit their local DEERS/RAPIDS office to obtain a new Common Access Card because the CAC is too old and/or does not contain the PIV Auth certificate.

- 5) In the ActivClient menu, select **<Tools> -- <Advanced> -- <Make Certificates Available to Windows>**.

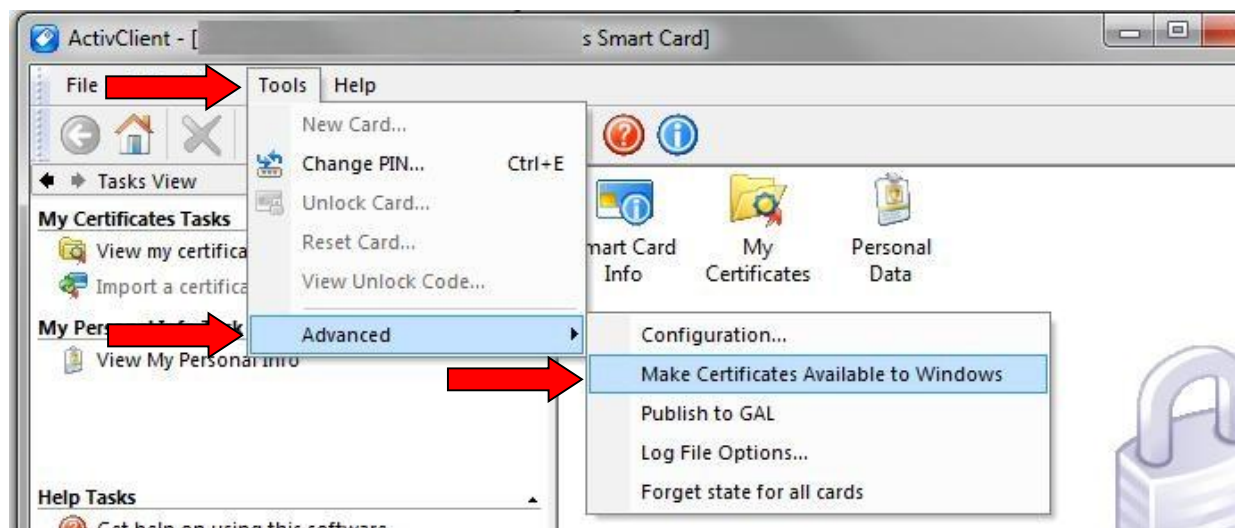


Figure 24. Making certificates available to Windows

**IMPORTANT NOTE:** The reason for activating the PIV Authentication certificate is that each dual persona user **must use** the PIV Auth certificate **to authenticate** to Enterprise Email. As a dual persona individual, **you will always use this certificate to authenticate to Enterprise Email**. The email certificate will still be used for signing and encrypting email. The PIV Auth cert is for authentication only!

**NOW, REPEAT THIS PROCESS FOR YOUR OTHER CAC...**

## 5 Why is the PIV Authentication certificate required?

The use of PIV Authentication certificates is required in order to distinguish between two different accounts (for each persona) of a given individual. This normally occurs whenever a DoD individual has two active CACs, either physically has two CACs or when the Defense Manpower Data Center (DMDC) records indicate that two CACs for the individual are both still valid (because a 'termination' transaction for the first one has not been received before the 'issue' transaction for the second one was processed). For example, a civilian who retires on Friday and returns the following Monday as a contractor will often get their new CAC on Monday (or sometimes even the week before) yet the retirement transaction from the civilian personnel system doesn't complete and flow across to DMDC until later that week. In this case the system indicates the individual has two CACs and two personas for a few days. The issue does not depend on having the same DoD organization for both CACs, it only matters on the electronic records indicating that two (or more) CACs are still valid for the individual (regardless of their organization). It also doesn't matter whether one persona was in an organization that is not using DEE. The PIV Auth cert is necessary to distinguish between the two personas of the individual.

## 6 What can be done to make the PIV Authentication requirement "go away"?

You can't. The important phrase to understand is "Once PIV Auth, always PIV Auth".

Once an individual is required to use the PIV Authentication certificate to authenticate to enterprise services provided by DISA, the user will **always be required to use the PIV Authentication certificate**, even after they only have one CAC. The enterprise system can identify when a duplicate entry exists, and so both records are changed from using the email certificate to using the PIV Authentication certificate (because the credentials provided by the email certificates of an individual are identical and the system cannot distinguish between them using the email certificates). When a particular records goes away, the system doesn't run through all 4.3 million other records trying to find a related record that has the same beginning portion of the electronic credential, and then figure out how to "reset" the remaining record.